False Load Attack to Smart Meters by Synchronously Switching Power Circuits

Yongdong Wu, Binbin Chen, Jian Weng, Zhuo Wei, Xin Li, Bo Qiu, and Niekie Liu

***Abstract*—In the electric energy metering process, current and voltage are sampled periodically and simultaneously, and then used to calculate the energy consumption. This paper presents a simple yet powerful attack to the above metering mechanism such that the calculated energy consumption is made far away from the actual one. Specifically, an adversary switches on/off the power circuit at the meter's sampling rate. If the meter samples the circuit at the circuit-off (or circuit-on) time, the measured energy consumption is much lower (or higher respectively) than the actual one. Unlike the state-of-the-art false load injection attacks, the present attack is immune to the well-known cryptographical countermeasure that builds a secure and time-stamped channel between the meter and the central system. We implemented a low-cost device to attack a simulated electric energy meter. According to the experiment results, the attack method is effective. Moreover, we propose a countermeasure on the present attack and demonstrate its effectiveness.**

***Index Terms*—Smart meter, Cyber-physical system security, False load attack, IGBT**

I. Introduction

As an important type of equipment for electric utility companies, electric energy meters are installed at customers' premises to measure the power consumption. The meters are read regularly to bill the customers at domestic, commercial and industrial level [1]. In early days, analog electromechanical energy meter is the dominant form. Albeit it is simple, the analog meter is inconvenient as the electricity utility companies have to read the meters manually.

Manuscript received ...; revised ... ; accepted ... The work was partly funded under the Energy Innovation Research Programme (EIRP, Award No. NRF2014EWT-EIRP002-040), administrated by the Energy Market Authority (EMA), Singapore; partly supported by the research grant for the Human-Centered Cyber-physical Systems Programme at the Advanced Digital Sciences Center from Agency for Science, Technology and Research (A∗STAR), Singapore; and partly supported by Guangdong Innovative and Entrepreneurial Research Team Program (No. 2014ZT05D238), and the National Natural Science Foundation of China under Grant No. 61402199, U1636209, 61472165, 61373158, U1636101, and U1736211. The associate editor coordinating the review of this paper and approving it for publication was ... Corresponding author: Jian Weng.

Y. Wu is with Institute for Infocomm Research, Singapore (email: wuyd007@qq.com).

B. Chen is with Advanced Digital Sciences Center, Singapore (e-mail: Binbin.chen@adsc.com.sg).

J. Weng is with Department of Computer Science, Jinan University, Guangdong, China, 510630 (e-mail: cryptjweng@gmail.com).

Z. Wei is with Huawei International Pte Ltd, Singapore (e-mail: phdzwei@gmail.com).

X. Li is with Sinocloud Wisdom Pte Ltd, Beijing, China, 100176 (e-mail: lixin@yunkouan.com).

B. Qiu is with Hebei University of Technology, China (e-mail: sfighter@126.com)

N. Liu is with Nexwah Technology Pte Ltd, Singapore (email: nikkieliu@nexwah.com)

With the advance of information and communication technologies, electric utilities are making steady progress in upgrading their customers' analog meters with digital smart meters [2]. As smart meters can send the measured consumption data remotely via a customer-operator communication channel, it not only facilitates the energy measurement process, but also enables new applications such as demand forecasting [3], dynamic tariff [4], and load management [5]. A number of countries have already made substantial investments in smart meter deployment [6]–[8], and the market for smart meters is expected to grow quickly at a CAGR (Compound Annual Growth Rate) of 9.34% from 2017 to 2022 [9].

To realize the advanced billing and energy management services, smart meters are equipped with high-precision AFE (Analog Front End) circuits, MCU (Micro-Controller Unit) and sophisticated data processing software [10], where AFE and MCU may be integrated together (e.g, Texas Instruments' MSP430AFE family) or separated (e.g., Atmel's 78M6612) [11]. In either case, a smart meter periodically obtains the instantaneous samples of the current/voltage of the load, and then uses the samples to calculate the electricity frequency, power factor, energy consumption, etc [12].

The metering process is subject to physical and/or cyber attacks that exploit various security flaws of meters via meter tampering, bypassing, or other unlawful schemes. For instance, an attacker can attach magnets to the meters to saturate the current and/or voltage transformers, compromise the meter software, or tamper with the traffic of communication channel between meters and the utility's central system [13], [14]. The attacks not only reduce the revenue of the electric utilities [15], [16], they may even have bad impact on the demand forecasting, pricing strategy, the power generation/schedule mechanism and power supply stability.

Nowadays, there are several countermeasures on these known attacks. The first is to detect whether the physical values (e.g., magnetic readings) are within a reasonable range; the second is to ensure software integrity protection by monitoring the state of the meter's firmware [17]; and the third is to deliver meter readings via a secure data communication channel (e.g., as specified in IEC 62351 [18]). Thanks to extensive efforts on enhancing the security of meters [19], the risk of these known attacks to smart meters can be mitigated effectively.

This paper presents a novel false load attack that is immune to all the above countermeasures, and can effectively incur a large amount of measurement error of a smart meter. The proposed new attack exploits the fundamental design in the electric metering mechanism. Specifically, we consider an attacker who is able to switch a power main line (or its

branch) measured by a smart meter in a manner that is synchronous with the meter's current measurement actions. For example, when the meter samples the current through a circuit, the attacker switches the circuit off such that the measured instantaneous current is 0. When the meter does not sample the circuit, the attacker switches on the circuit to consume electricity. Doing so leads to effective electricity theft. In addition, it can also destabilize the whole power grid if the false measurement is used to realize load control or management [20], [21]. In order to defeat the present attack, we propose a novel countermeasure that introduces randomness into the meter's sampling timing such that the attacker will have difficulty to synchronize his circuit-switching with meter sampling. To demonstrate the applicability of the present attack, a prototype using an Insulated Gate Bipolar Transistor (IGBT) is designed and built. The experiments show that the present attack is viable and the proposed countermeasure is effective.

The remainder of this paper is organized as follows. Section II provides the background related to the present attack. Section III presents the novel false load attack and analyzes the attack feasibility, parameters, and performance. Section V presents the prototype implementation and experiment results. Finally, Section VI draws conclusions.

Nomenclature

ADC: Analog to Digital Converter
AFE: Analog Front End
IGBT: Insulated Gate Bipolar Transistor
MCU: Micro-Controller Unit
OCXO: Oven-Controlled Crystal Oscillator
PWM: Pulse Width Modulation
PCB: Printed Circuit Board
TCXO: Temperature-Compensated Crystal Oscillator

T_{ON}: Circuit-ON duration in a sampling cycle
T_{OFF}: Circuit-OFF duration in a sampling cycle
$T_{G_{ON}}$: IGBT gate-ON duration in a sampling cycle
$T_{G_{OFF}}$: IGBT gate-OFF duration in a sampling cycle
$T_{d_{ON}}$: IGBT rising time
$T_{d_{OFF}}$: IGBT falling time
Δ: Threshold value (lower bound) for circuit-OFF duration
τ: Sampling period of an electric meter
ρ: Duty cycle of a gate PWM signal
W: Energy consumption
$p(t)$: Real power value at time t
$i(t)$: Current value at time t
$v(t)$: Voltage value at time t

II. Preliminaries

To provide the background for the present attack, this section first briefly describes the design of a smart meter and the energy measurement principle. Then it introduces IGBT, which is used to realize the present attack.

A. Smart meter

Fig.1 shows the diagram of a smart meter, which includes AFE, MCU, display, and communication module for remote reading [22].

An AFE consists of voltage input circuit, current input circuit and filter circuit, where the voltage input circuit attenuates the actual voltage to satisfy the measurement upper boundary, the current input circuit converts the current to a voltage through a current transformer or resistor, and the filter circuit reduces the gain and phase errors. Besides, it may have ADC (Analog to Digital Converter) to sample the current and voltage, and calculate the power, energy consumption, etc [10].

Through a dedicated interface (e.g., Serial Peripheral Interface), an MCU communicates with AFE and performs data processing. It also conducts the necessary configuration of AFE, such as calibrating meter gain, and compensating phase errors. In addition, the MCU outputs the measurement results on display and sends the readings via a communication module.

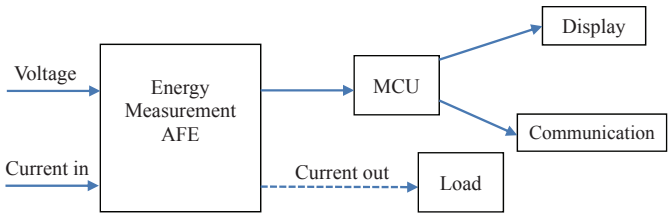

Fig. 1. The basic elements of a smart meter for measuring the power consumption of a load [23]. When the present attack is started, the dash line will be manipulated by the attacker such that current in/out is changed.

B. Real power measurement

As the real power is the target of the adversary in this paper, we focus on its measurement principle. As introduced in [24], real power is calculated as the product of the instantaneous current measurement and the instantaneous voltage measurement, sampled in a synchronized manner (e.g., at a sampling rate of 6400Hz or sampling period $\tau = 156.25\mu s$). Mathematically, the instantaneous real power $p(t)$ is the product of voltage $v(t)$ and current $i(t)$, i.e, $p(t) = v(t) \times i(t)$. The energy consumed (and billed) for a given time interval is the integral of the instantaneous real power $p(t)$. Considering a single-phase meter for example, we obtain the energy consumption over a period from time 0 to $K\tau$ as

$$W = \int_0^{K\tau} p(t)dt \approx \sum_{j=1}^{K} v(j\tau)i(j\tau)\tau \tag{1}$$

For a revenue billing application, smart meters, just like analogy meters, should meet accuracy standards, such as ANSI C12.20 [25]. Therefore, the accuracy of both current and voltage measurements are critical in the power measurement process.

C. IGBT

As shown in Fig.2, an IGBT is a terminal semiconductor device for conducting current I_c in one direction [26]. Concretely, the circuit is turned on if the gate signal V_{GE} is sufficiently high (e.g., 15V), or turned off if $\mathrm{V_{GE}} \leq 0$. Thanks

to the advance of high speed semi-conductor technologies, the fifth generation IGBTs (e.g., IKW40N65F5FKSA1) [1] have very short switching time such that IGBT can be used to switch circuits sufficiently fast to match typical smart meter sampling frequency.

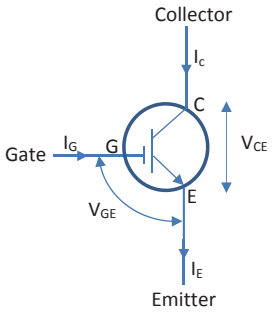

Fig. 2. IGBT diagram. If $V_{GE} \geq 15V$ (i.e., gate-ON), the circuit between collector and emitter will be on (i.e., circuit-ON), $V_{CE} \approx 0$ and $I_C (\approx I_E)$ is large. But if $V_{GE} \leq 0V$ (i.e., gate-OFF), the circuit will be off (i.e., circuit-OFF), $I_C \approx 0$ and $I_E \approx 0$.

III. False Load Attack

According to the meter structure and measurement principle as described in Section II, the accuracy of the energy measurement relies on the accuracy of both the current and voltage measurements. Also, by the Nyquist-Shannon sampling theorem, the discrete sequence of samples can represent the continuous-time electricity signal, if the electricity signal contains no frequencies higher than half of the sampling frequency, which generally holds in a trusted environment. However, as we will show below, an attacker is able to invalidate this underlying assumption in the digital metering process, and incur a large error of the smart meter, by synchronously switching the circuit.

A. Security model

In the present attack, the adversary aims to reduce the meter's accuracy without changing the meter, input line of the meter, and communication channel between meter and the utility's central system. To this end, the adversary is assumed to be

- able to insert or find an IGBT switch between the output end of the target meter and the input end of the load;
- able to control the IGBT switch to turn on/off the target electricity circuit;

The above assumptions can be realized in two cases. In the first case, the attacker installs a new IGBT switch device into the power circuit. For example, an electricity user can do so to steal electricity. Note that, the attacker can carry out this in a rather stealthy and convenient manner by modifying a normal power indoor extension with a controllable IGBT switch, and can easily unplug and hide the modified power extension to avoid detection. In the second case, as IGBT is popularly used in many power rectifiers / inverters [27]–[30], the attacker may be able to exploit those existing IGBT switches to launch the attack.

In either case, if the IGBT controller is under the control of the attacker via some means[2], the attacker is able to switch the power circuit even remotely. This posts a potential risk that an attacker may be able to conduct such attacks on a large number of sites remotely, hence causes a grid-wise impact. For simplicity, the following will elaborate the first case with a resistor load, unless otherwise stated.

B. Attack method

To launch the attack, an attacker can change the power circuit by adding an IGBT into an existing circuit, as shown in Fig.3. The IGBT is inserted between the load and the smart meter, and it is controlled by a digital gate signal. In the attack, the attacker will use an MCU to send periodic circuit-OFF signals to the IGBT gate such that the circuit is switched off when the meter is sampling the current reading. Because the circuit is open, the sampled current value is zero (or close to zero if there is some hysteresis), i.e., the current $i(t) \approx 0$ at the sampling time of t. Hence, according to Eq.(1), the power meter readings for the total consumption will be

$$W \approx \sum_{k=1}^{K} v(k\tau) i(k\tau) \tau \approx 0$$

Nonetheless, at any non-sampling time, the IGBT gate signal is gate-ON such that the load can consume energy during these moments. As a consequence, the energy measurement can be made much lower than the actual consumption. On the contrary, if the meter always samples the circuit when the gate is ON, the energy measurement can be made much higher than the actual consumption.

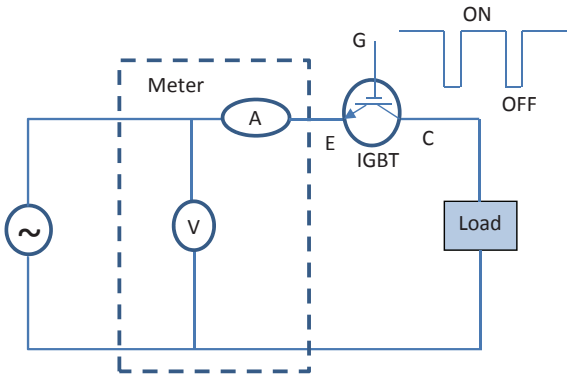

Fig. 3. Circuit diagram of the present attack. For the IGBT, its collector C links to the load, the emitter E links to the output of current sensor, and its gate G links to a digital controller (omitted in the figure). The attacker uses the controller to issue periodic pulse signal that is synchronized with the meter reading time.

Due to the dynamic characteristics of capacitive and inductive elements in the circuit, it takes some times (e.g., tens of

[1]IGBT-High speed 5 FAST IGBT in TRENCHSTOP^{TM} 5 technology co-packed with RAPID 1 fast and soft anti parallel diode, see http://www.mouser.com/ds/2/196/Infineon-IKW40N65F5-DS-v01_02-EN-219455.pdf.

[2]For instance, the controller is installed by the attacker, has a backdoor at the manufacturing stage, or has a compromised and/or wireless network interface [31].

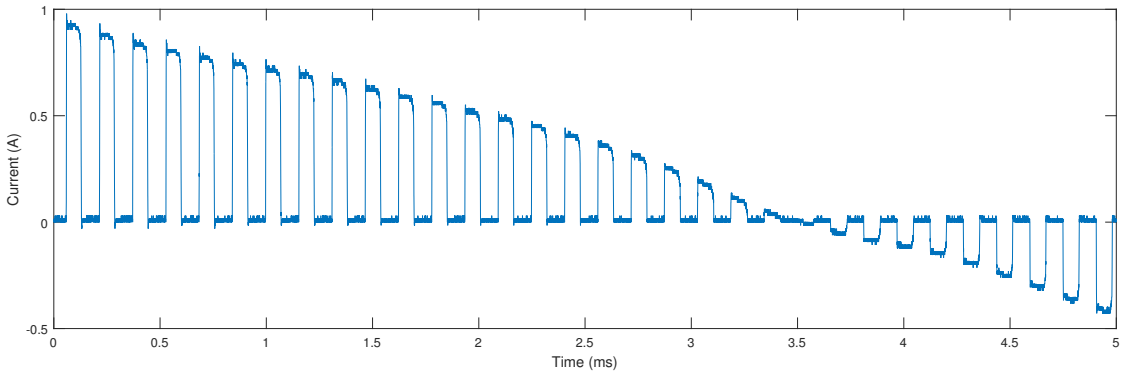

Fig. 4. Current sample sequence when the power line is switched at 6400Hz (i.e., sample period is 156.25μs), 50% duty cycle.

nanoseconds) to reduce the load current to 0 after the IGBT gate voltage is changed from high to low. Thus, the width of gate-OFF signal shall be big enough to complete circuit-OFF operation. For instance, suppose that the duty cycle[3] is 50%, the current value can become 0 when gate-OFF signal is low, as shown in Fig.4.

C. Synchronization method

In order to successfully attack the meter, the gate signal must synchronize with the meter sampling process. However, the sampling signal is internal to the meter and is not available to the attacker. Therefore, an attacker shall find other means to determine whether the gate signal synchronizes with the sampling signal or not.

There are two general types of meter implementations to determine the sampling time. One is continuous metering and the other is zero-crossing metering. The former is to take the periodic samples in a continuous manner over time without referring to the underlying electricity signals, while the latter aligns the periodic samples with the zero-crossing time of the measured voltage signals. For instance, the popular power measurement chip RN8302B [32] offers two modes: One is fixed sampling rate 6400Hz for nominal frequency 50Hz power grid (in China, Europe etc) and cross-zero sampling 7699Hz for nominal frequency 60Hz power grid (e.g., in USA). The attacker shall take different synchronization methods for different metering modes.

1) Synchronization for continuous metering: As shown in Fig.5, a smart meter is able to provide its real-time power measurements on its display screen. In addition, it may provide the consumption data with a front panel interface (e.g., RS-232 serial, optical port or wireless) which is used by field engineers to calibrate / reconfigure the meter on site.

Therefore, an attacker is able to determine whether the attack succeeds or not by reading the display or the meter's communication interface. In this attack process, the attacker can use a simple control loop to initialize its attack. Basically, after sending the gate-ON/gate-OFF signals at the the meter sampling frequency (but with randomly chosen phase offset),

[3]In a PWM ((Pulse Width Modulation)) signal, duty cycle is the ratio between high-voltage time and PWM period.

Fig. 5. An example smart meter with an optical port, which is able to output power consumption.

the attacker can read the meter's power measurement and if the meter's power measurement is close to 0, the attack already succeeds. Otherwise, the attacker knows that there is a phase difference between its attack signal and the sampling process. If the circuit-ON duty cycle is around 50%, the attacker can simply shift its gate signal by 0.5τ to make the meter sampling time fall into the circuit-OFF instead of circuit-ON period, hence making the power measurement close to 0. If the frequency of both the meter and the attacking device are stable and match exactly, the attacker does not need to further monitor the meter reading after the synchronization is achieved. We will discuss how to cope with slight difference of frequency in the subsection IV-B.

2) Synchronization for zero-crossing metering: In a zero-crossing meter, there is a circuit for detecting the zero-crossing point of the electricity voltage. Upon the detection of the zero-crossing point, the meter will start to periodically sample the electricity till its next zero point. Thus, besides the attack process mentioned in Subsection III-C1, the attacker needs to be able to launch a closed-loop attack process so as to provide long-time synchronization between the meter's sampling process and the IGBT's circuit ON/OFF process.

IV. Discussions

In the present attack, the duty cycle, the stability of the crystals, and the tuning mode of the compromised devices have significant impact on the attack performance. This section discusses these parameters and then addresses countermeasures.

A. Duty-cycle selection

With reference to Fig.3, the load is connected with the IGBT and meter in series. Denote circuit-ON duration within a sampling cycle as T_{ON}, and circuit-OFF duration within a sampling cycle as T_{OFF}. A meter sampling period is $\tau = T_{ON} + T_{OFF}$. Now we consider the impact of the rising / falling delay between the gate signal ON/OFF time and the actual circuit's ON/OFF time. Denote $T_{d(on)}$ as the rising time and $T_{d(off)}$ as the falling time of the IGBT, and denote $T_{G_{ON}}$ and $T_{G_{OFF}}$ as the IGBT gate-ON / gate-OFF duration in a sampling cycle respectively. We should set $T_{G_{OFF}} = T_{OFF} + (T_{d(off)} - T_{d(on)})$, and circuit-ON time is $T_{G_{ON}} = \tau - T_{G_{OFF}}$.

The objective of the attack is to ensure that the meter will sample the power circuit within the circuit-OFF duration of T_{OFF}. Thus, in order to incur the largest measurement error, T_{OFF} shall be made as small as possible. That is to say, $T_{OFF} \geq \Delta$, where Δ is the admissible threshold to handle the device variation in crystal frequency, the synchronization error tolerance, and the capacity or delay of IGBT control circuit. Thus the circuit-OFF signal time

$$T_{G_{OFF}} \geq \Delta + (T_{d(off)} - T_{d(on)}) \tag{2}$$

and the circuit-ON signal time

$$T_{G_{ON}} = \tau - T_{G_{OFF}} \leq \tau - \Delta - (T_{d(off)} - T_{d(on)}) \tag{3}$$

Thus, to launch a successful electricity theft attack, the duty cycle of the gate signal should be

$$\rho = \frac{T_{G_{ON}}}{\tau} \leq 1 - \frac{\Delta + T_{d(off)} - T_{d(on)}}{\tau} \tag{4}$$

As an illustrative example, assume $T_{d(on)} = 1\mu$s, $T_{d(off)} = 30\mu$s, the sample period is $\tau = 156.25\mu$s (i.e., sampling frequency is 6400Hz), and the threshold $\Delta = 10\mu$s. If the attacker chooses $T_{OFF} = 0.5\tau = 78.125\mu$s (note that T_{OFF} cannot be less than Δ), the IGBT gate-ON duration is $T_{G_{ON}} = 156.25 - 78.125 - (30-1) = 49.125\mu$s and the IGBT gate-OFF duration $T_{G_{OFF}} = 107.125\mu$s. Thus, the duty cycle of the gate signal is $\rho = 107.125/156.25 = 68.56\%$ which is higher than the targeted circuit-ON duty cycle of 50% because $T_{d(off)} > T_{d(on)}$.

B. Sensitivity analysis

The present attack takes effect when the gate signal is synchronized with the meter sampling signal. As the attacker has no control on the stability of the meter's crystal (and sometime no control over the attack device's crystal when the attack reuses in-situ hardware), it is necessary to investigate the effect on synchronization due to the practical stability issues of crystal frequency.

1) Instability of a meter's crystal: Suppose the meter's crystal frequency f is uniformly and randomly distributed over an interval of $[f_0 - rf_0, f_0 + rf_0]$ for some predefined value r, with mean f_0 (or period $\delta = 1/f_0$). Denote the frequency $f_i = f_0 + r_i f_0$ for some $r_i \in [-r, r]$, and the period is $T_i = \delta + n_i$ at the ith cycle, where the period deviation

$$n_i = \frac{1}{f_i} - \frac{1}{f_0} = \frac{f_0 - f_i}{f_0 f_i} = \frac{r_i}{f_i} = \frac{r_i \delta}{1 + r_i} \tag{5}$$

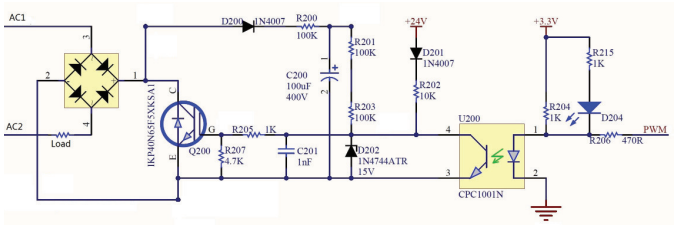

Fig. 6. Schema of the attack device. The control signal PWM is sent from MCU.

Thus, after the meter runs l crystal cycles, the total time error is

$$e_l = \sum_{i=1}^{l} (T_i - \delta) = \sum_{i=1}^{l} n_i = \delta \sum_{i=1}^{l} \frac{r_i}{1 + r_i} \tag{6}$$

Assume that the stability of a crystal is high, $|r_i| \ll 1$. Thus Eq.(6) can be simplified as

$$e_l \approx \delta \sum_{i=1}^{l} r_i \tag{7}$$

The right side of Eq.(7) can be approximated as a normal distribution $\mathcal{N}(\mu_l, \sigma_l^2)$ according to the central limit theorem, where mean $\mu_l = 0$ and variance is

$$\sigma_l^2 = \frac{l r^2 \delta^2}{3} \tag{8}$$

or $\sigma_l = \sqrt{\frac{l}{3}} \cdot r\delta$. For instance, assume the clock frequency is 8MHz (or $\delta = 1/8\mu s$), and $r = 30$ ppm (i.e., 30×10^{-6}) for a crystal oscillator with a medium level of precision[4],

$$\sigma_l = \sqrt{\frac{l}{3}} \times 30 \times 10^{-6} \times 1/8 = \sqrt{l} \times 2.165 \times 10^{-6}$$

Suppose the sampling period is $T = 156.25\mu$s (i.e., sampling rate is 6400Hz), and duty cycle 50%, or 78.125μs. Assume initial time is at the center of duty cycle, to deviate from the duty cycle with a probability of 70% (or 1-sigma),

$$78.125/2 = \sqrt{l} \times 2.165 \times 10^{-6}$$

we have $l \approx 3.32 \times 10^{14}$ cycles. i.e., it takes $l\delta \approx 4.15 \times 10^7$ seconds to lead to the attack failure due to the instability of meter's crystal frequency.

2) Inconsistence of meter's crystals: Due to the difference of crystals, the sampling period also varies across meters (albeit within a small interval). Denote the crystal period of meter as T_m and the crystal period of an attack device as $T_a < T_m$. Assume the initial sampling time is at the middle of the circuit-OFF duration, and the sampling time will move to the circuit-ON time after q sampling period, we have

$$\frac{T_{OFF}}{2} = q \times \frac{\tau}{T_m} \times (T_m - T_a) \tag{9}$$

[4]One important factor that destabilizes the crystal oscillator's frequency is the change of environmental temperature. Thus it is possible to considerably improve the stability of the oscillator by applying temperature compensation technologies on the crystal oscillator module. TCXO (Temperature-Compensated Crystal Oscillator) or OCXO (Oven-Controlled Crystal Oscillator) are two popular compensated crystal oscillator which offer excellent short-term stability to limit the influence of temperature fluctuation [33].

Thus the running time of a successful attack is

$$q\tau = \frac{T_m T_{OFF}}{2(T_m - T_a)} \geq \frac{T_m \Delta}{2(T_m - T_a)} \tag{10}$$

For example, assume the difference $T_m - T_a = 10^{-7}\delta$, $\tau = 156.25\mu$s, $T_{OFF} = \tau/2 = 78.125\mu$s, it takes $q\tau = 400$ seconds to lead to the attack failure. Therefore, in comparison with the crystal instability discussed in Subsection IV-B1, the inconsistence of meter crystals has much higher impact on the attack performance. Therefore, the attacker shall compensate the crystal difference of attack device so as to reduce deviation between the sampling period and IGBT gate period. The compensation can be realized by tuning the attack period T_a based on a closed-loop feedback control by checking the attack success / failure patterns using the meter readings.

C. Admissible threshold

With reference to Subsections IV-A and IV-B, the admissible threshold Δ is used to tolerate the uncertainty of crystals. When admissible threshold Δ becomes smaller, the duty cycle can be chosen higher according to Eq.(4), such that the difference between the actual energy consumption and the measurement by the meter will be higher. However, smaller Δ requires more accurate synchronization between attack frequency and sampling frequency according to Eq.(10).

D. Cyber-attack to the grid

In the present attack, electricity theft may happen if an attacker controls circuit switches such that the measured energy consumption is different from the actual one. While this can already cause direct economic impacts, a more serious situation may occur if the meter readings are used in the DR (Demand-Response) [34] or LFC (Load-Frequency Control) [21]. In this case, the attacker may be able to attack the whole power grid by launching remote false data injection attack to a large number of meters using the proposed method. By abusing a large number of controllers (e.g., cases in Subsection III-A) such that the measurement error is sufficiently big, the DR or LFC becomes erroneous, and consequently the smart grid will suffer from big disturbance, even instability.

The present attack is able to incur measurement error within the interval (-100%, 100%) of actual load consumption if the duty cycle is 50%. Hence, the more the number of compromised devices, the higher the total error interval. To reduce the required number of compromised devices, the attacker may flexibly choose attack parameters so as to tune the attack from time to time. Such attack flexibility can be achieved as follows.

1) Tuning duty cycle for variable attack amplitude: The present attack is able to incur different levels of erroneous readings in the meter. Specifically, if the meter sampling point is always at the circuit-OFF time, the reading is lower than the actual value. On the contrary, if the meter sampling point is always at the circuit-ON time, the readings is higher than the actual value. The final effect depends on the occurrence ratio of these two cases. Thus, if an attacker wants to incur a target time-variant error within this range, he can achieve so by adjusting the duty cycle of the gate signal as shown in Eq.(4) from time to time.

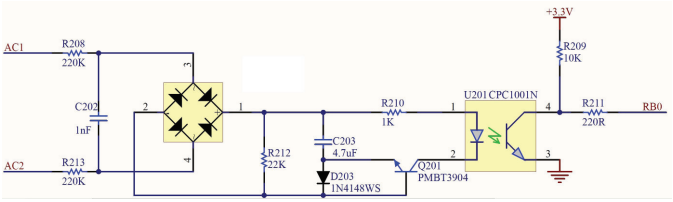

Fig. 7. Zero-crossing detection circuit. The voltage zero-crossing signal is sent to MCU port RB0.

2) Adjusting period deviation for different attack duration: Besides tuning the attack amplitude of the measurement errors, the attack can change the error period by changing the deviation between the meter sampling period and gate-changing period of the attack device according to Eq.(9) or Eq.(10).

E. Countermeasures

When a smart meter is under the present attack, its voltage samples are the same as the utility input and its current samples are about 0. As these samples are the same as the normal load-free setting, the meter is unable to identify the attack. Thus, new countermeasure needs to be introduced to existing smart meters to defend against the attack.

In order to launch the attack, the circuit switch frequency must be higher than the cut-off frequency of the AFE. Otherwise, the attack effect will be filtered out. However, as there is some delay in the IGBT switching on/off circuit, the circuit switch frequency is restricted such that the circuit cannot be completely switched if the cut-off frequency is high. Therefore, one countermeasure is to increase cut-off frequency of the AFE by increasing the capacitance of the AFE filter or meter sampling rate.

Another countermeasure is to sample the circuit randomly rather than periodically. As random sampling makes it difficult to achieve and maintain synchronization between the meter sampling process and the circuit-ON/OFF timing, the present attack is deterred in principle.

V. Implementation and Experiment

A. Attack device

We have implemented a proof-of-concept attack device. The design diagram of our attack device is shown in Fig.6, which includes a full-bridge rectifier, an IGBT, and a transistor output opto-coupler for protecting the low-voltage circuit. The input PWM signal generated from an MCU pin is used to produce the gate signal which controls the circuit ON/OFF timing. Fig.7 shows the zero-crossing detection design to adapt to the zero-crossing metering process presented in Subsection III-C1. Correspondingly, Fig.8 is the PCB (Printed Circuit Board) prototype of Fig.6 and Fig.7.

B. Experiment configuration

As shown in Fig.9, the experiment configuration includes the attack device, two load resistors linked in series (400Ω in total), and a simulated meter (see Subsection V-C below). The MCU is PIC18LF25K50 from Microchip^{TM}, the crystal for

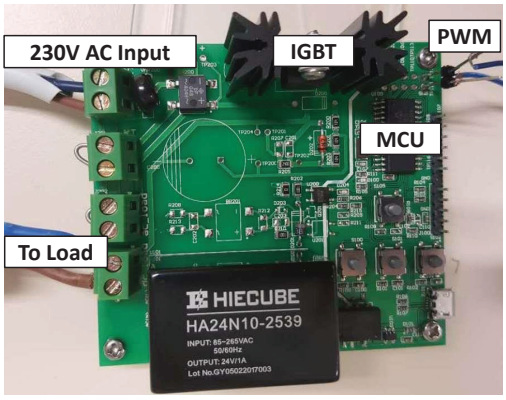

Fig. 8. The attack device prototype. The IGBT and MCU are the key components in the attack device. By switching on/off the 230V AC input, the attack device affects the power usage at the load and the measurements at the meter.

MCU is 16MHz with 30ppm, the meter sampling frequency is 6400Hz, and the mains electricity runs at 50Hz and 230Volt.

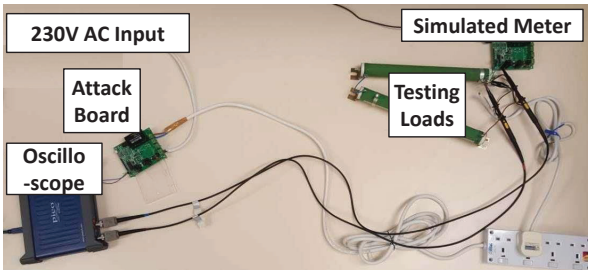

Fig. 9. Experiment configuration. It includes the attack device, the resistive load and a simulated meter.

C. Simulated meter

In order to expose the internal status of a smart meter for illustrating the attack process, we design a simulated meter, which follows the same design principle in Fig.1 [23]. Specifically, the simulated meter has an MCU which has an ADC to sample the voltage (equivalently, current) of a small resistor, the MCU will output the measured current/voltage. As the attack device and the simulated meter have the same components, their hardware designs are the same. The oscilloscope is used to display the measured samples, PWM and gate signal.

Smart meters can use different measuring sensors such as including resistive shunt, current transformers (CTs) [35] or Rogowski coils [36]. As resistive shunt has traditionally been the most commonly-used current sensing technique for residential and other low-to-medium-power applications, it is adopted as a current measurement tool for simulating smart meter in the experiments[5].

[5]In order to filer high-frequency noise, the commercial energy meter usually have a low-pass filer in the AFE. In the reference design [10], the filter is constructed with resistor $R = 1000\Omega$ and capacitor $C = 33$nF. As its cut-off frequency is $\frac{1}{2\pi RC} = 4822.87$Hz which is slightly lower than the gate-signal frequency 6400Hz, the filter is able to alleviate the attack performance to some extent, but does not prevent the attack in principle.

D. Control circuit response

Fig.10 shows the response of the IGBT control circuit, where the solid line is the measurement of load current AC1, and the dotted-dash line indicates the digital value of pin 4 of part U200 (i.e., the inverse of PWM from MCU) in Fig.6. When the PWM signal is turned to be 0, the circuit delay (rising time) is merely 1μs. However, when the PWM is changed to 1, the circuit delay (falling time) is about 30μs. Thus, the turn-off delay is longer than the turn-on delay.

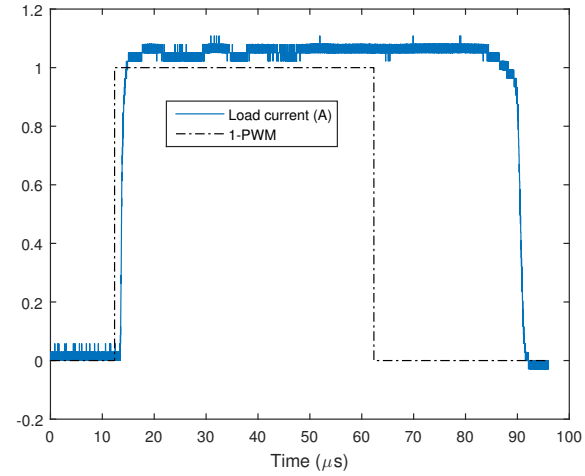

Fig. 10. IGBT response characteristics for on/off switching. IGBT turns on a circuit quickly, but takes a longer time to turn off the circuit.

E. Attack results

1) Instantaneous current value: Fig.11 shows the current waveform when the meter always samples the load current at the circuit-OFF time. In this case, the current sampling value of the meter will be almost zero. Hence, the calculated power consumption is almost zero too.

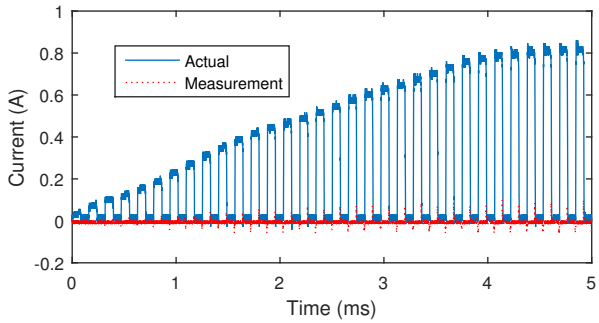

Fig. 11. When a meter samples the circuit at the circuit-OFF time, the current sample value is 0. The circuit's duty cycle is 50%.

On the contrary, Fig.12 shows the current waveform when the meter always samples the load current at the circuit-ON time. In this case, the sampling value of the meter will be almost the same as the real instantaneous power value. Since the meter uses these power values for those circuit-OFF duration (which actually consumes no power), the calculated

energy consumption over time will be higher than the actual one.

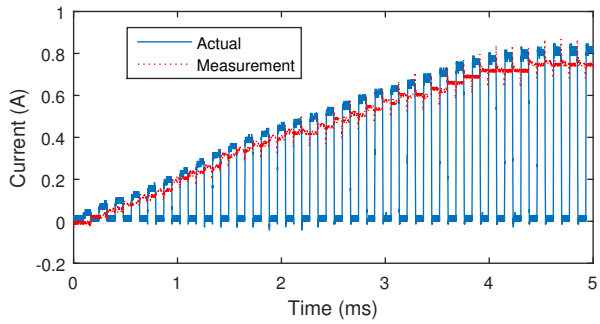

Fig. 12. When a meter samples the circuit at the circuit-ON time, the transient sample value is the same as actual value. The duty cycle is 50%.

2) Erroneous power value due to duty cycle: When the attack device and the meter do not synchronize precisely, Eq.(10) shows that the measured power changes periodically. This can be observed in both Fig.13 and Fig.14.

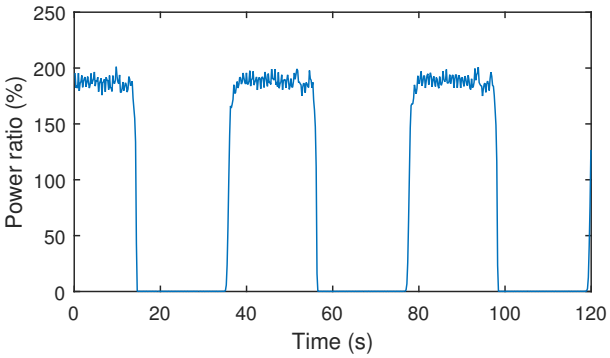

Fig. 13. The IGBT gate signal has 50% duty-cycle, at an expected sample period 156.25μs. The y-axis shows the ratio between the measured power and the actual power. Clearly, the range of the error ratio is about {-100%, 100%}

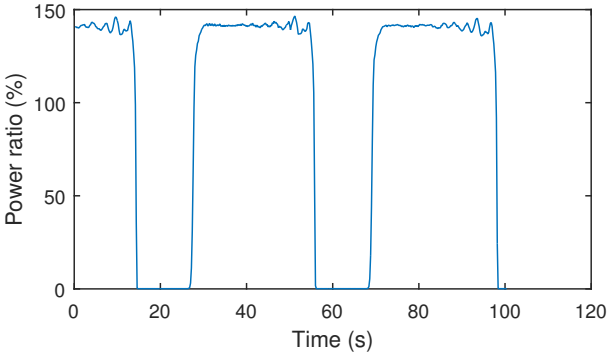

Fig. 14. The IGBT gate signal has 66.6% duty-cycle, at an expected sample period 156.25μs.

Therefore, if an attacker observes the meter through the meter screen or optical interface, he can find abrupt changes of the meter readings periodically. This can be used by the attacker to readjust its attack device's signal phase. For example, when an attacker sees that the measured power is larger than the actual power its load consumes (e.g., around the 37th second in Fig.13), the attacker can instruct the attack device to shift the gate signal to quickly revert back to the attack mode (i.e., the low part of the curve in Fig.13) such that the meter readings become low again.

3) Error cycle: Eq.(10) shows that the period of the measured power is proportional to $(T_a - T_m)^{-1}$, the inverse of the difference between the meter sampling frequency and IGBT gate signal frequency. That is to say, when the difference is smaller, the period of the error of the measured power will increase. It can be seen by comparing Fig.13 and Fig.15.

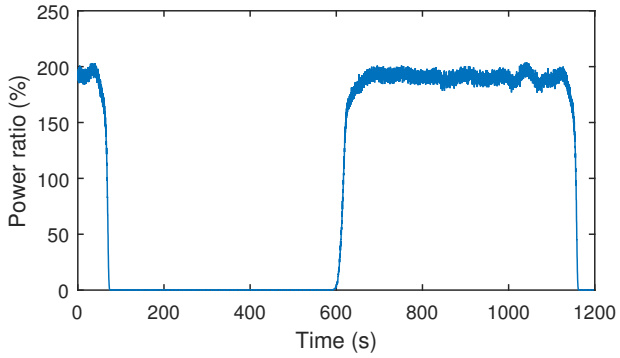

Fig. 15. The IGBT gate signal has 50% duty-cycle, at an expected sample period 156.25μs. In comparison with Fig.13, its period is larger because its synchronization error between the meter sampling frequency and gate signal frequency is smaller, but the range of the error ratio is the same, i.e., about {-100%, 100%}.

F. The effect of countermeasure

When the sampling period of the device is changed randomly within an interval $[0, 0.5\tau]$, the attack is deterred as shown in Fig.16, where the distribution of power ratio is mean 1.0026, and standard deviation 0.028. That is to say, the actual power consumption is almost the same as the measured one, and hence the measurement error is very small.

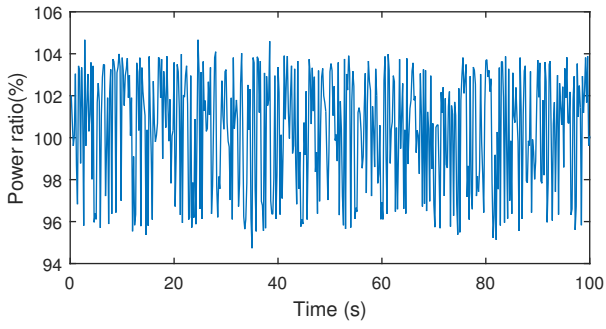

Fig. 16. The effect of countermeasure on the attack in Fig.15. The actual power consumption is almost the same as the measured one.

VI. Conclusions

Energy measurement is a fundamental requirement in smart grid. It not only affects the revenue of the electric utilities, but

also may have impact on the stability of the power grid. By exploiting a flaw of the metering principle, this paper presents a false load attack to make the meter reading far away from its true value. The attack is implemented and validated on a simulated energy meter. As the attack is very effective, of low cost, can be launched in a stealthy manner, and can reduce the power consumption bill significantly, it may be used in real world. Moreover, as there may be many rectifiers/inverters in the generation, transmission, distribution, and consumer sides of the power grid, the present attack may be employed to attack the smart grid when the attacker is able to compromise their controllers.

As the attack compromises neither the meter nor the communication channel, it has advantage over the start-of-the-art false load injection attack which can be defeated with standard security measures. To defeat the present attack, the meter should adopt random sampling or use higher sampling frequency.

REFERENCES

[1] S. S. Raza, M. Ahmad, and M. S. Perveiz, "Performance Of Energy Meters Under Harmonic Generating Environment," Science International (Lahore), 26(5):2063-2069, 2014.

[2] Institute for Electric Efficiency, "Utility-Scale Smart Meter Deployments, Plans, and Proposals," The Edisoon Foundation, May 2012.

[3] Y. Cheng, C. Xu, D. Mashima, V. L. L. Thing, and Y. Wu, "PowerLSTM: Power Demand Forecasting Using Long Short-Term Memory Neural Network," *in Proc IEEE Conference on Advanced Data Mining and Applications*, pp.1-6, 2017.

[4] D. Fischer, B. Stephen, A. Flunk, N. Kreifels, K. B. Lindberg, B. Wille-Haussmann, and E. H. Owens, "Modeling the Effects of Variable Tariffs on Domestic Electric Load Profiles by Use of Occupant Behavior Submodels", *IEEE Transactions on Smart Grid*, vol. 8, no.6, pp. 2685-2693, 2017.

[5] C. P. Mediwaththe, E. R. Stephens, D. B. Smith, and A. Mahanti, "A Dynamic Game for Electricity Load Management in Neighborhood Area Networks," *IEEE Transactions on Smart Grid*, 7(3):1329-1336, 2016.

[6] L. Alejandro, C. Blair, L. Bloodgood, M. Khan, M. Lawless, D. Meehan, P. Schneider, and K. Tsuji, "Global Market for Smart Electricity Meters: Government Policies Driving Strong Growth," Office of Industries, U.S. International Trade Commission, ID-037, June 2014.

[7] Edison Foundation Institute, "Utility-Scale Smart Meter Deployments: Building Block of the Evolving Power Grid," Sept. 2014. Access on 14 Feb. 2018. http://www.edisonfoundation.net/iei/publications/Pages/publications.aspx?category=Report

[8] N. Strother, "In Japan, Smart Meters Accelerate," 01 May 2014. Access on 14 Feb. 2018. https://www.navigantresearch.com/blog/in-japan-smart-meters-accelerate

[9] "Smart Meters Market worth 19.98 Billion USD by 2022," MarketsandMarkets.com. Access on 14 Feb. 2018. http://www.marketsandmarkets.com/PressReleases/smart-meter.asp

[10] S. English and D. Smith, "A Power Meter Reference Design Based on the ADE7756," Analog Devices, Inc., 2001.

[11] L. H. Goldberg, "Accurate Power Measurement in Smart Meters, Part I: Design Considerations," 25 Apr. 2012, Digi-Key Electronics. Access on 14 Feb. 2018. http://www.digikey.com/en/articles/techzone/2012/apr/accurate-power-measurement-in-smart-meters-part-i-design-considerations.

[12] C. L. King, "AN994: IEC Compliant Active-Energy Meter Design Using The MCP3905A/06A," Microchip Technology Inc., 2009.

[13] M. Costache, V. Tudor, M. Almgren, M. Papatriantafilou, and C. Saunders, "Remote Control of Smart Meters: Friend or Foe?" *in Proc. Eur. Conf. Computer Network Defense*, pp. 49-56, 2011.

[14] O. Kosut, L. Jia, R. J. Thomas, and T. Long, "Malicious Data Attacks on the Smart Grid," *IEEE Trans. Smart Grid*, 2(4):645-658, 2011.

[15] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, and X. (S.) Shen, "Energy-Theft Detection Issues for Advanced Metering Infrastructure in Smart Grid," *Tsinghua Science and Technology*, 19(2):105-120, 2014.

[16] Deloitte, "Using Analytics to Crack Down on Electricity Theft," 02 Dec. 2013. Access on 14 Feb. 2018. http://deloitte.wsj.com/cio/2013/12/02/using-analytics-to-crack-down-on-electricity-theft/

[17] O. Fatemieh, M. LeMay, and C. A. Gunter, "Reliable Telemetry in White Spaces using Remote Attestation," *in Proc ACM Annual Computer Security Applications Conference*, pp.323-332, 2011.

[18] International Electrotechnical Commission (IEC), "Smart Grid - Core IEC Standards." Access on 14 Feb. 2018. http://www.iec.ch/smartgrid/standards/

[19] E. E. Queen, "Smart Meters and Smart Meter Systems: A Metering Industry Perspective," EEI-AEIC-UTC White Paper, Mar. 2011.

[20] R. Tan, H. H. Nguyen, E. Y. S. Foo, X. Dong, D. K. Y. Yau, Z. Kalbarczyk, R. K. Iyer, and H. B. Gooi, "Optimal False Data Injection Attack Against Automatic Generation Control in Power Grids," *ACM/IEEE International Conference on Cyber-Physical Systems*, pp.1-10, 2016.

[21] Y. Wu, Z. Wei, J. Weng, X. Li, and R. H. Deng, "Resonance Attacks on Load Frequency Control of Smart Grids," *IEEE Transactions on Smart Grid*, pp.1-13, 2017. DOI: 10.1109/TSG.2017.2661307.

[22] K. S. K. Weranga, S. Kumarawadu, and D. P. Chandima, "Smart Metering Design and Applications," Springer publisher, Chap. 2, 2014.

[23] L. H. Goldberg, "Accurate Power Measurement in Smart Meters, Part 2: Specifying Components," 01 Aug. 2012, Digi-Key Electronics. Access on 14 Feb. 2018. http://www.digikey.sg/en/articles/techzone/2012/aug/accurate-power-measurement-in-smart-meters-part-2-specifying-components.

[24] A. Devine and O. Cerid, "Single Phase Digital Power Meter Reference Design Designer Reference Manual," DRM040, Freescale Semiconductor, Inc, 2003. Access on 14 Feb. 2018. www.nxp.com/files/microcontrollers/doc/ref_manual/DRM040.pdf

[25] L. A. Irwin, "A High Accuracy Standard for Electricity Meters," Schneider Electric Industries SAS. Apr. 2011.

[26] S. Abedinpour and K. Shenai, "Insulated Gate Bipolar Transistor," Power Electronics Handbook (3rd Edition), Chap.5, Academic Press, 2011.

[27] K. Thiyagarajah, V. T. Ranganathan, and B. S. R. Iyengar, "A High Switching Frequency IGBT PWM Rectifier/Inverter System for AC Motor Drives Operating from Single Phase Supply," *IEEE Transactions on Power Electronics*, 6(4):576-584, Oct. 1991.

[28] M.-Y. Chang, R.-S. Ou, and Y.-Y. Tzou, "DSP-based Fuzzy Control of Bilateral IGBT PWM DC-to-AC and DC-to-DC Converters for Battery Energy Storage System," *in Proc. International Conference on Industrial Electronics Control and Instrumentation*, pp. 1117-1122, 1993.

[29] B. Singh, B.N. Singh, A. Chandra, K. Al-Haddad, A. Pandey, and D.P. Kothari, "A review of single-phase improved power quality AC-DC converters," *IEEE Transactions on Industrial Electronics*, 50(5):962-981, Oct. 2003.

[30] L. M. A. Caseiro and A. M. S. Mendes, "Real-Time IGBT Open-Circuit Fault Diagnosis in Three-Level Neutral-Point-Clamped Voltage-Source Rectifiers Based on Instant Voltage Error," *IEEE Transactions on Industrial Electronics*, 62(3):1669-1678, March 2015.

[31] K. Yamamoto, F. Ichihara1, K. Hasegawa, M. Tukuda, and I. Omura, "60 GHz Wireless Signal Transmitting Gate Driver for IGBT," *in Proc IEEE International Symposium on Power Semiconductor Devices & IC's*, pp.133-136, 2015.

[32] "Introduction to RN8302B," Sunshine Science Pte Ltd. Access on 14 Feb. 2018. http://en.sfkj-tech.com/cp3_2/productId=98.html

[33] J. Bausch, "TCXO vs. OCXO," 02 Aug. 2011. Access on 14 Feb. 2018. https://www.electronicproducts.com/Passive_Components/Oscillators_Crystals_Saw_Filters/TCXO_vs_OCXO.aspx

[34] A. Paverd, A. Martin, and I. Brown, "Security and Privacy in Smart Grid Demand Response Systems," *in proc International Workshop on Smart Grid Security*, Lecture Notes in Computer Science 8448, pp. 1C15, 2014.

[35] Working Group C-5 of the Systems Protection Subcommittee of the IEEE Power System Relaying Committee, "Mathematical Models for Current, Voltage, and Coupling Capacitor Voltage Transformers," *IEEE Trans. on Power Delivery*, 15(1):62-72, 2000.

[36] Y. Wang, J. Li, Y. Hu, R. An, Z. Cai, and R. He, "Analysis on the Transfer Characteristics of Rogowski-coil Current Transformer and Its Influence on Protective Relaying," *Energy and Power Engineering*, 5, pp.1324-1329, 2013.